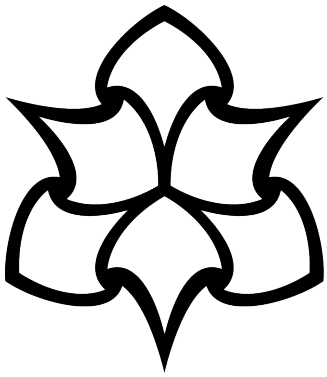


Building Covert Timing Channel of the IoT-Enabled MTS Based on Multi-Stage Verification

Chen Liang, Thar Baker, *Senior Member, IEEE*, Yuanzhang Li, Raheel Nawaz, and Yu-An Tan

***Abstract*— Although the global shipping industry is experiencing a productivity revolution due to the adoption of IoTs (Internet of Things), the dependence on complex data transmission and interactive centers is also increasing, which makes the IoT-enabled Maritime Transportation Systems (MTS) one of the most valuable but vulnerable industries against network security attacks. To guarantee the transmission security of confidential data, an important alternative in an untrustworthy IoT-enabled MTS is to apply the covert timing channels. This paper mainly introduces the construction of covert timing channel with low bit shifting rate and high reliability by multi-stage verification and error correction. For the covert timing channel schemes realized by active packet loss, the packet loss noise interferes with the channel's reliability. However, due to the constraints of stealthiness, the active packet loss ratio during covert communication is low, so more effective reliable strategies are needed to reduce noise interference. In the excellent scenario, when the bit error rate is lower than 0.08%, the transmission performance is kept at 0.49 bps. In the good scenario with strong network noise, although this method loses some performance, it can still maintain the transmission performance of 0.2 bps under the condition of bit error rate less than 1%, which effectively proves the effectiveness of multi-stage verification and error correction.**

***Index Terms*— Covert timing channel, IoT-enabled MTS, multi-stage verification, robustness.**

I. Introduction

FOR decades, the data security and privacy of shipping industry are suffering from cyber-attacks aiming at money theft, information interception and causing disruption [1]. The Petya malware attack in 2017 made headlines in the global media, causing massive damage and requiring Maersk to rebuild its network of 4000 servers and 45000 PCs, resulting in a loss of about $300 million. In 2018, Barcelona and Santiago ports were attacked by blackmail software, and the Geneva headquarters of mediterranean shipping company was attacked by malware on April 10. Investigation of the incident found that there was no data theft and the attack affected a limited number of computer systems. With the pervasively adoption of IoT into the industry field, It is increasingly challenging to transmit data safely and secretly over wireless communication channel [2], [3], and the key agreement schemes and data encryption schemes have been proposed in that case [4]–[7]. Although efforts have been done to ensure the data transmission security, the encryption-based methods cannot resist adversaries from inferring information from communication patterns to obtain transmission information. The privacy of the critical information and confidential data may be utilized if the opponent is skillful enough to obtain and decrypt the coded data [8]–[11]. Thus, covert timing channel is an alternative to enhance data protection capability.

With the expansion of data transmission applications, covert channel in the data transmission environment is the current research hotspot [12]–[16]. In the network environment, the construction of covert timing channel is based on packet traffic. Covert storage channel (CSC) utilizes redundant fields in TCP packet header, such as sequence number field, to transmit secret messages [17]. Correspondingly, the rival destroys the storage channel through data rewriting or normalization [13], [18]. For VoIP and other applications, the packet transmission frequency is high, and the covert channel based on storage content is also of high performance [19], [20]. Combined with steganography and other data embedding methods, the CSC also has good effect on video and multimedia applications [20], [21] Different from the CSC, the covert timing channel (CTC) is designed on fine tuning of the characteristics of packet transmission and does not change the data content. Therefore, there is no exposure risk of the temporal covert channel when the data field is under monitored. Since the CTC has the same transmission characteristics as the host channel, simultaneous interpreting data content or detecting transmission characteristics cannot identify the existed covert traffics. Therefore, CTC is suitable for scenes with strict concealment requirements [22]–[24].

VoLTE has been widely used in the communication systems and industries as an LTE call solution. It is a global interoperability solution that provides advanced communication functions. To guarantee the transmission's concealment, the active packet loss rate is low. By analyzing the packet capture data,

Manuscript received June 5, 2021; revised August 18, 2021; accepted October 1, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant 62072037, Grant U1936218, and Grant 61876019; in part by the Fundamental Research Funds for Beijing Universities of Civil Engineering and Architecture under Grant X20069; and in part by the Research Fund of Beijing Information Science and Technology University under Grant 2021XJJ49. The Associate Editor for this article was A. K. Bashir. *(Corresponding authors: Thar Baker; Yuanzhang Li.)*

Chen Liang is with the School of Information Management, Beijing Information Science and Technology University, Beijing 100192, China (e-mail: 20202441@bistu.edu.cn).

Thar Baker is with the Department of Computer Science, University of Sharjah, Sharjah, United Arab Emirates (e-mail: tshamsa@sharjah.ac.ae).

Yuanzhang Li and Yu-An Tan are with the School of Computer Science and Technology, Beijing institute of Technology, Beijing 100081, China (e-mail: popular@bit.edu.cn; tan2008@bit.edu.cn).

Raheel Nawaz is with the Department of Operations, Technology, Events and Hospitality Management, Manchester Metropolitan University, Manchester M15 5RN, U.K. (e-mail: r.nawaz@mmu.ac.uk).

Digital Object Identifier 10.1109/TITS.2021.3118853

the packet dropout rate of VoLTE video channel is higher than the QCI target value of LTE network, and the SNR of CTC is low. The packet dropout types of VoLTE are divided into random packet loss noise with length of 1 and continuous packet loss noise. For the low density random packet loss noise, the noise and signal can be effectively distinguished by embedding the check information; while for the continuous packet loss noise, a single set of check information cannot be effectively identified, so it needs to be identified by redundant data in multiple groups of check information. The method of constructing CTC based on multiple parity check is mainly studied. In the three levels of codeword, symbol and mapping matrix, the check and error correction process is added respectively to reduce the noise intensity layer by layer. In this method, three levels of verification are used, i.e., inter symbol check, codeword self check and inter symbol check. Combined with hash digest algorithm, Cyclic Redundancy Check (CRC) hash algorithm and XOR check algorithm, it achieves a lower bit error rate in excellent scene, and effectively reduces the average BER in good scene. This method's innovations are as follows:

1) A CTC construction method based on multi-stage verification and error correction is proposed, which can effectively reduce the bit error rate;

2) The verification and error correction method including three levels of inter symbol check, codeword self check and inter symbol check is designed to reduce the noise level layer by layer;

3) The proposed scheme supports transmission parameter adjustment to enhance robustness and ensure transmission performance;

4) The experimental results show that by adjusting the transmission metrics of the proposed scheme, the transmission capability, bit error rate and undetectability can be balanced, and the availability and effectiveness of the covert channel are effectively improved.

The remaining paper is divided and illustrated with this order: section 2 introduces the interference of network noise on covert timing channel, robust strategy based on inter symbol check, motivations, and section 3 gives the proposed schemes overview and introduces each parts of the covert channel. Section 4 mainly introduces the proposed multi-stage verification and error correction scheme, and section 5 illustrates the implementation and evaluation results of the proposed scheme. Section 6 provides the related works about wireless covert channel schemes in IoT environment. Finally, section 7 includes a brief conclusion.

II. Background

This section introduces the related background of this method, including the interference mode of network noise to the CTC, and the reliability strategy based on inter symbol check. Among them, the interference of network noise on covert timing channel is analyzed, and the solution is proposed. Based on the robust strategy of inter-codeword verification, a verification relationship between codewords is proposed to improve the utilization of verification information.

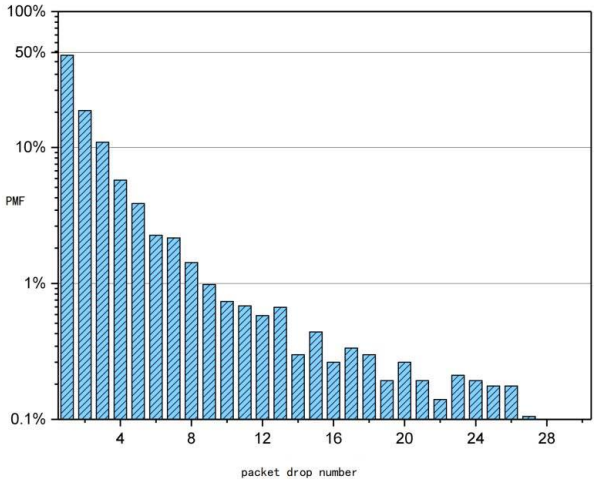


Fig. 1. The Probability Mass Function(PMF) for Packet drop number of the VoLTE video streams.

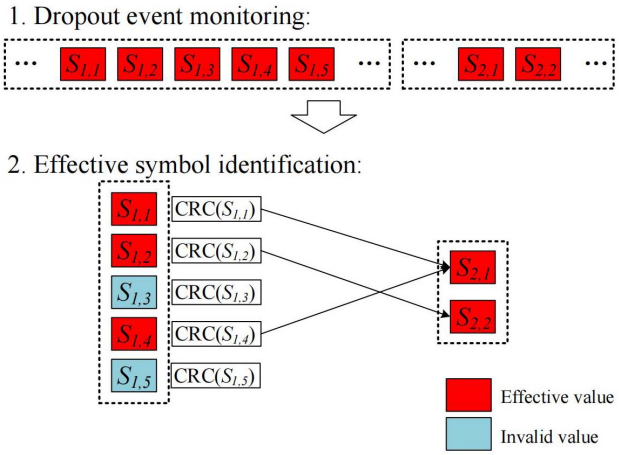


Fig. 2. The influence of continuous packet loss on error correction process.

A. Interference of Network Noise on Covert Timing Channel

It can be obviously concluded from Fig.1 that the random packet loss rate while $length = 1$ is about 50% in VoLTE video call, and the rest are continuous packet loss events. Through CRC error detection code and other ways, the discrete random packet loss noise can be well suppressed. For the interference of continuous packet loss noise, the probability of mismatching in the verification process is high, the accuracy rate of codeword identification is reduced, and finally, the bit error rate is increased.

As shown in Fig.2, in the case of packet loss in continuous reading, the verification capability is degraded. The first group S_1 is the data symbol to be verified, and the second group S_2 is the candidate verification symbol. $CRC(S_{1,I})$ was calculated in turn and compared with $S_{2,J}$. Because the check symbol is only a part of CRC hash result, the probability of collision is high. Only part of the network noise can be identified. At the same time, due to the lack of additional information, the noise cannot be further identified, and finally error code appears.

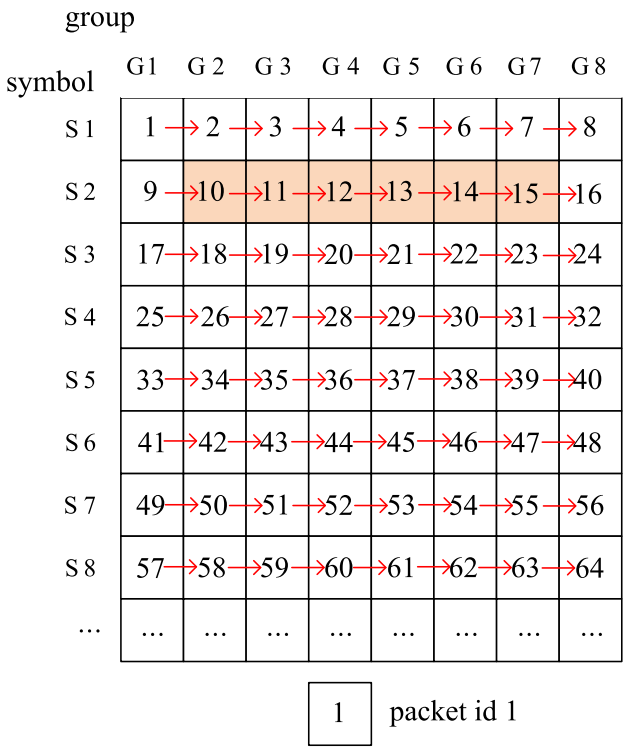


Fig. 3. The symbol packet sequence number mapping matrix: Elements in the matrix represent for the packet numbers; Column number of is the group number, and row numbers corresponds to the symbols.

In the ideal case, when there is noise in the data codeword and there is no noise in the check codeword, the error probability is $1/L_{Codeword}$, which has the effective identification ability. In the actual scene, the verification codeword is interfered by noise, and the identification failure in Fig.1 occurs.

It is a feasible way to deal with this kind of noise by dispersing the continuous packet loss into different groups and using the check ability of each group to reduce the noise interference. As illustrated from Fig.3, the elements in the matrix consists of the packet numbers, the column number of the matrix is the group number, and the row number of the matrix corresponds to the symbol. When continuous packet loss noise, such as 10 $\sim$ 15, is processed by the mapping matrix, the noise is allocated to packet 2 $\sim$ 7. The mapping matrix pattern is beneficial to make full use of the verification capability of each group and improve the utilization rate of verification resources.

B. Robust Strategy Based on Inter-Codeword Check and Verification

In the time implicit channel robustness strategy, rate free coding such as fountain code is included, and the real message content is restored by combining the redundant data between multiple codewords [25]. In blockchain technology, each block is embedded with the hash value which is obtained according to the previous block, so when the chain reaches a certain scale, the starting block is fully verified [26]. In the active packet loss CTC, due to the uneven distribution of noise, using the information in the low noise stage to verify the information

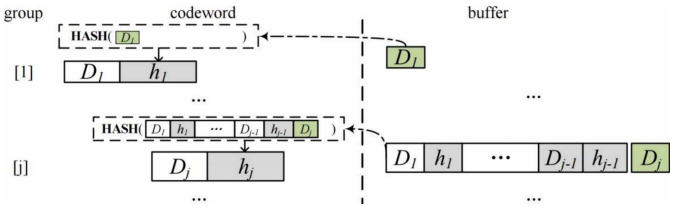


Fig. 4. The inter code check structure, the inter-codeword check information is applied to verify the correctness of received codeword.

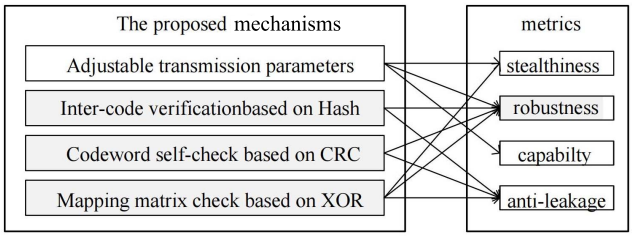


Fig. 5. The main checking mechanisms adopt in the proposed scheme and its affections on CTCs channel parameters.

in the high noise stage can further improve the utilization rate of the verification information.

As shown in Fig.4, the inter-codeword check block h_j records the hash value of the data buffer. With the randomness and certainty of hash function, with the advance of receiving process, the correctness of received codeword is verified through the inter-codeword check information in the received codeword. Even if some codewords cannot be identified by noise interference, cascade verification is realized with the help of effective information in other groups.

Salt adding operation is implemented in hash summary during the calculation process, and the confidentiality of covert timing channel is improved by combining user shared information and RTP random fields. Because the listener can not get the salt value, the inter-codeword check block h_j cannot be recovered correctly, and the inter-codeword check relationship is protected. Thus, when there is noise interference, the listener cannot distinguish the noise and signal, and the secret message is protected.

C. Motivation

In this method, the basic modulation method is active packet loss, and the modulation results are hidden in the network noise. The method of multi-stage verification and error correction can effectively de noise, improve robustness and reduce bit error rate. In the process of multi-stage verification and error correction, salt adding and randomization are introduced to enhance the randomness and confidentiality.

As shown in Fig.5, the key points of this method include adjustable transmission parameters, hash-based inter-codeword check, CRC- based codeword self-check as well as XOR based mapping matrix check. Among them, the adjustable transmission parameters mainly solve the balance between the undetectability, robustness and transmission performance. This method needs to sacrifice performance to ensure robustness, so all aspects are balanced by adjusting transmission

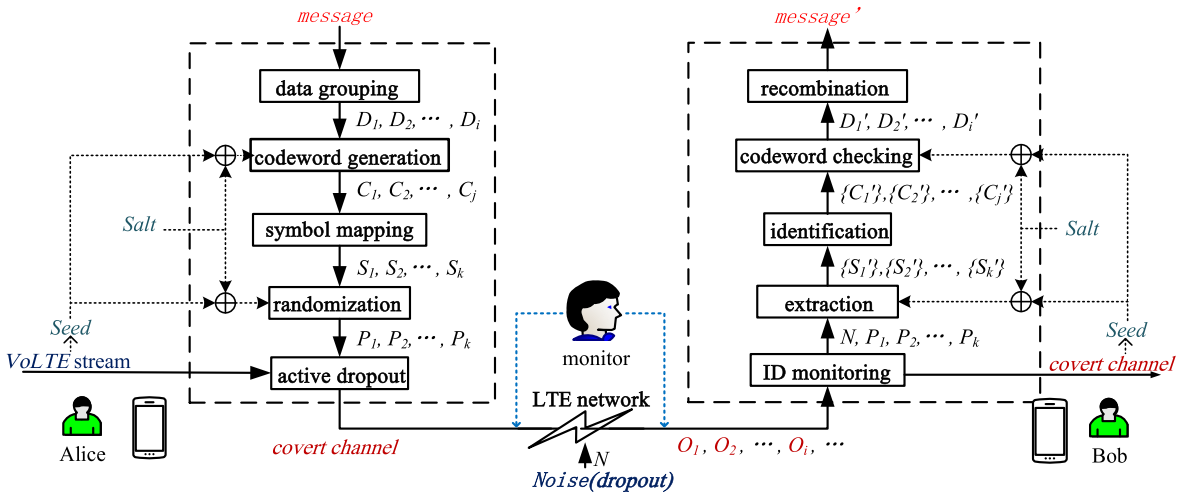


Fig. 6. Overview of the covert timing channel based on multi-stage verification and error correction, Alice and Bob represent for sender and receiver, respectively.

parameters. The inter-codeword check based on hash and the codeword self check based on CRC mainly enhances the reliability (robustness) of the covert timing channel and the confidentiality of the hidden message. The mapping matrix checking based on XOR can improve the robustness by constructing the mapping matrix with verification ability.

III. System Design

This section gives an overall description of the construction method of the CTC. First, it introduces the design architecture, then introduces the modulation process and data conversion process, and finally introduces the demodulation process and data conversion process.

A. Overview

The design overview of the CTC construction method is illustrated in Fig.6. For the covert channel sender Alice and the covert channel receiver Bob, it is necessary to avoid the listener to transmit the secret messages. In order to ensure the confidentiality of the message, both parties agree to share the variable salt, which is used to enhance the randomness of the transmission process. The sender first groups the hidden messages to get the message block D_i. Next, according to the random field seed in the shared salt and RTP, the codeword generation process calculates the inter-codeword check information and codeword self check information to form codeword C_j. Then, referring to the mapping matrix, the codeword is mapped to the symbol S_k, that is, the relative packet loss position. The symbol randomization process adds a random offset to each set of symbols and converts it to the packet sequence number P_k to be discarded.

A monitor is adopt between sender side and receiver side, and the capability of monitor is to simulate the adversary which keeps accessing and detecting the abnormal flows introduced by the proposed covert channel. By adopting the monitor, we set the schemes adversary model as bellows:

Adversary model: We assume that the main structures and specific designs of the covert channel realized by active packet loss have been known to the adversary. Since the NIQE will be seriously affected, the adversary cannot modify the majority of packet traffics and we also assume that the adversary cannot obviously disturb the transmission of overt traffic even if the existence of covert channel is detected. Moreover, we also assume that the key and encrypt algorithm adopted during the stealth communication is secure enough and only shared by the channel senders and receivers.

The host channel is VoLTE video channel. The covert timing channel is constructed after the packets with specific sequence number are discarded in the active packet loss process. After transmission through LTE network, the receiver performs the covert channel demodulation operation. The listener is located in LTE network and can monitor and control all packets.

In the process of demodulation, the receiver monitors the data packet transmission and gets the lost packet's serial ID P_k. Referring to mapping matrix and verification rules, the symbol extraction process converts $\{P_k\}$ to the candidate symbol set $\{S_k'\}$. In the process of symbol extraction, the random offset of each group of symbols is eliminated, and the shared salt and seed derived from RTP are used. In the codeword identification process, the $\{S_k'\}$ is converted into a candidate codeword, and the CRC based codeword self checking information in the codeword is verified, and the candidate codeword set $\{C_j\}$ in each group is output. In the inter-codeword verification and identification stage, the verification of the check relationship between codewords is carried out, and the combination with the maximum probability is selected, which is derived as the message block d_i'. Finally, the message blocks are recombined, the receiver gets the secret message, and the covert timing channel transmission is completed.

B. Modulation Phase

As shown in Fig.7, the data flow changes in the modulation process are mainly divided into five parts, which are basically

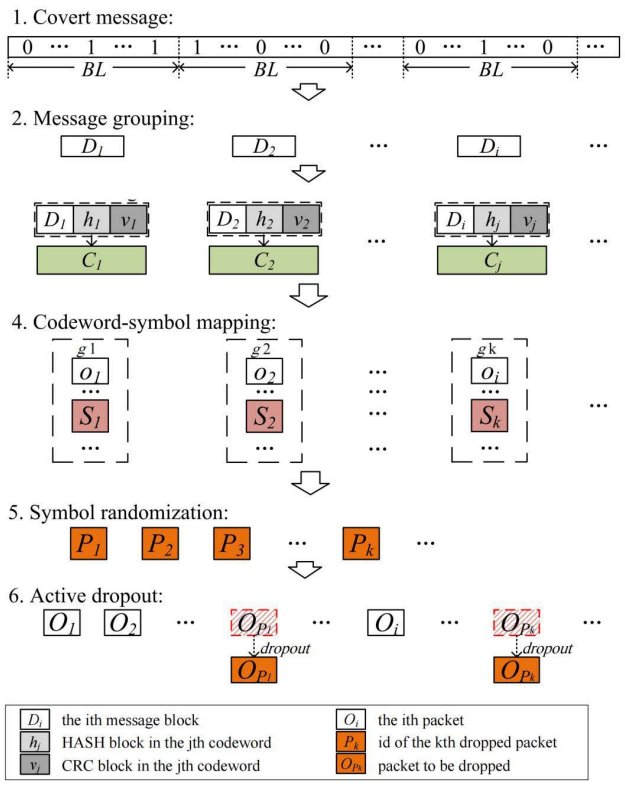


Fig. 7. Modulation flow of the proposed scheme: 1.secret messages grouping; 2. codeword mapping; 3. symbol randomization; 4. active dropout.

consistent with the process in the covert timing channel architecture. Firstly, the secret messages are grouped, and the length of each data block is BL, and the equal length data block $\{D_1, D_2, , D_i\}$ is obtained. Next, hash based inter-codeword check is calculated on the basis of each data block, and L_{HASH} bits are extracted from the summary results as H_j and spliced into the tail of d_i. For each $\{D_i//h_j\}$ combination, the CRC hash value is calculated, and L_{CRC} bits are extracted from the results as v_j. Finally, the Di, hj, vj are combined in order to obtain the codeword C_j. Therefore, the relationship between $L_{Codeword}$ and BL, L_{HASH} and L_{CRC} is shown in Eq. 1.

$$L_{Codeword} = BL + L_{HASH} + L_{CRC} \tag{1}$$

The codeword symbol mapping process converts the binary codeword C_j into the relative offset S_k in each group. During the mapping process, XOR check symbols are added, so the number of S_k is more than that of C_j. Next, the random number generator is iterated based on the input random number seed, and the random offset is added for each group of symbols. The pseudo-random number generator has the same random number sequence when the seeds are consistent, so the receiver can completely restore it. By combining the shared information of users and SSRC random field in RTP, it can ensure that the packet loss position is different each time, resist replay attack and enhance confidentiality. Finally, the symbol is converted into the serial number P_k of the data packet, which is discarded by the active packet loss process, and the modulation process ends.

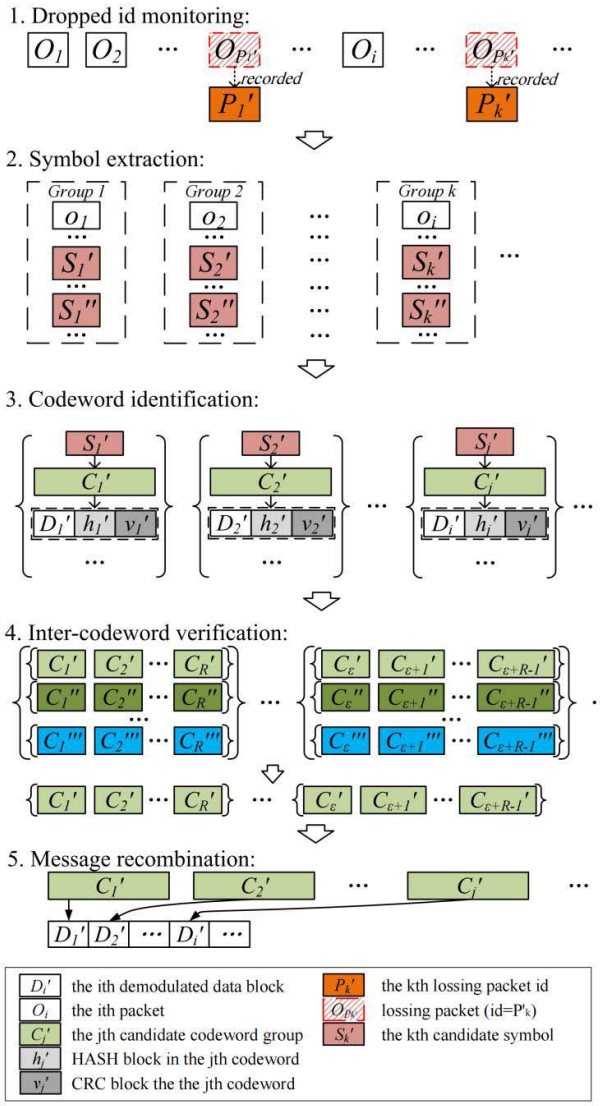


Fig. 8. Demodulation flow of the proposed scheme: 1. dropped packet id monitoring; 2. symbol extraction; 3. codeword identification; 4. inter-codeword verification; 5. message recombination.

C. Demodulation Phase

In Fig.8, the information flow for the demodulation process mainly includes five parts, corresponding to the demodulation process in Fig.6. The dropped packet's serial ID is analyzed. According to the vacancy of the serial ID, the dropped packet number P_k' is obtained. Because of the inevitable network noise, the candidate symbols of each group are set $\{s_k', s_k'' \cdot \cdot\}$

For the candidate symbols $\{s_k', s_k'' \cdot \cdot\}$, the pseudo-random number generator is iterated according to the random number seed to eliminate the random offset in the symbol. By verifying the XOR relation, the data symbols that conform to the rules are identified.

In the process of codeword identification, firstly, the v_j' part contained in the codeword is verified, and the candidate codewords that meet the rules are obtained. Next, the h_j' part in the codeword is verified. According to the mode of inter-codeword check, all codeword combinations are traversed. If the verification fails, the combination is invalid. Finally,

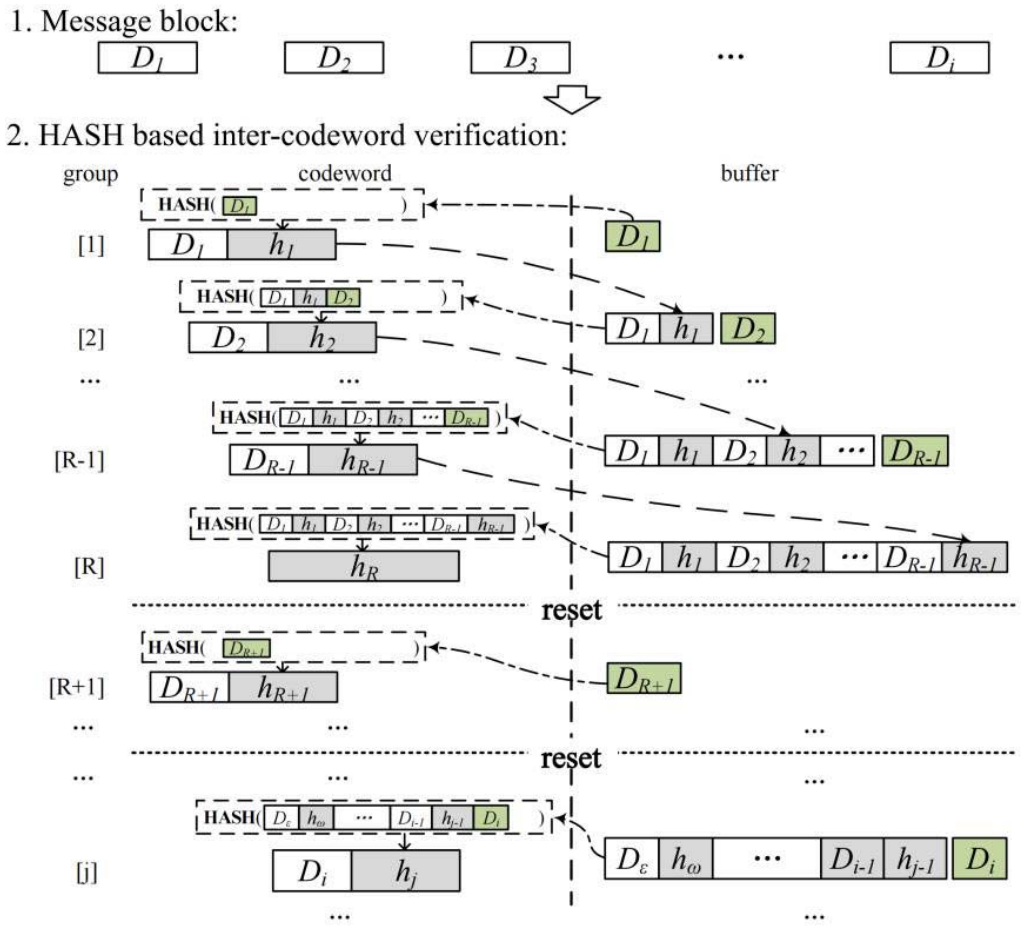


Fig. 9. The inter-codeword check based on Hash in the modulation phase.

a set of codeword combinations with maximum probability $\{C'_1, C'_2, \cdots, C'_j\}$ are obtained. In the final message reorganization process, the data blocks D_i in the codeword are combined in order to obtain hidden messages.

The covert timing channel construction method has the transmission synchronization ability, and can ensure the message order without synchronization clock. By combining inter symbol check, codeword self check, inter symbol check and mapping matrix, the noise intensity is reduced layer by layer, and the robustness of covert timing channel is improved.

IV. Multi-Stage Verification and Error Correction

This section introduces the multi-stage verification and error correction methods in this method, including hash based inter symbol check method, CRC-based codeword self-check method as well as XOR check based mapping matrix check method. The introduction of each method includes two aspects: modulation phase and demodulation phase.

A. Inter Code Check Method Based on Hash

The parameters involved in hash based inter code verification are L_{HASH} and R, salt shared by users and random seed derived from RTP. By establishing the verification relationship between multiple groups of codewords, the cascade verification between codewords is established.

1) Modulation Phase: In the modulation phase, the inter-codeword check based on hash is shown in Fig.9. To establish concatenated verification between codewords, it is necessary to maintain the transmit buffer to record the current content to be verified. In the initial stage, the buffer is empty. The first group of data block D_1 is added to the buffer, and hash (D_1) is calculated as H_1 to splice to the end of D_1, and h_1 is added to the buffer. According to the sequence of group number, the verification process is iterated in turn. When the group number is r, the data in the buffer has accumulated long enough to perform the reset operation. In the reset phase, a special check block h_R is generated, whose length is $BL + L_{HASH}$, and the buffer is cleared.

$$\omega = \left\lfloor \frac{j-1}{R} \right\rfloor \times R + 1 \tag{2}$$

$$\varepsilon = \omega - \left\lfloor \frac{\omega}{R} \right\rfloor \tag{3}$$

$$i = j - \left\lfloor \frac{j}{R} \right\rfloor \tag{4}$$

$$j = \left\lfloor \frac{i}{R-1} \right\rfloor \times R + (i-1) \tag{5}$$

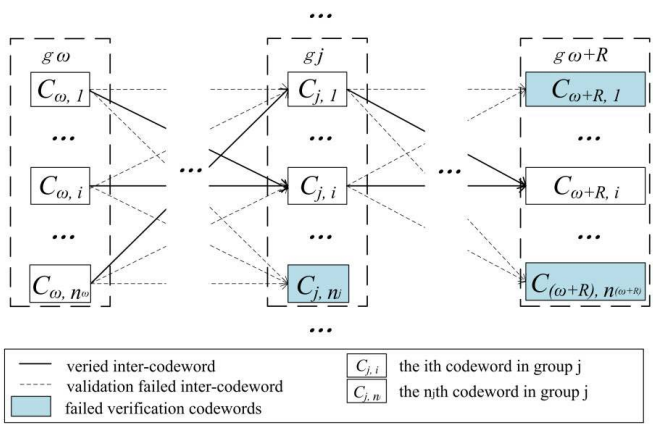


Fig. 10. Inter-codeword check based on HASH during the demodulation stage.

According to the reset period R, all inter symbol check blocks h_j are calculated in turn until the end. Due to the addition of additional check codewords in the reset phase, the corresponding relations between I and j in D_i and h_j are shown in Eq. 4 and Eq. 5. In Fig.9, the correlativeness of the reset start message block D_ε and the group number j, such as Eq. 2 and Eq. 3.

2) Demodulation Phase: In the demodulation phase, the inter symbol check based on hash is shown in 10, which is segmented according to the reset cycle R. the verification process in each cycle is carried out separately to reduce the calculation scale and prevent noise propagation. For the candidate codeword set $\{C'_1, \cdots\}, \{C'_2, \cdots\}, , \{C'_R, \cdots\}\}$, all feasible solutions form the directed acyclic graph. The starting point is $\{C'_1, \cdots\}$, and each edge in the graph corresponds to an association between codewords.

The demodulation process is similar to the graph traversal process. Starting from the starting point, all edges are verified. Only if the verification rules are met, the edges will be deleted from the graph. For the nodes of non $\omega + R$ group, when the node out degree is 0, it means that there is no successor node that meets the requirements. The node is judged as network noise and removed. Finally, when there is a path from the starting point to the node of group $\omega + R$, it is a possible combination of codewords. Under the interference of network noise, the candidate combination is not unique, and the path with the largest sum of nodes in all paths is selected as the final result.

B. Codeword Self Checking Method Based on CRC

Based on CRC, the correctness of $D_i//h_j$ is verified by setting CRC check block v_j in codeword C_j. This method is based on a single codeword, and there is no dependency between codewords, so the modulation and demodulation process is efficient.

1) Modulation Phase: In the modulation phase, the CRC based inter symbol self check process is shown in Fig.11. The codeword consists of D_i, h_j and v_j. The CRC based codeword check block is v_j, and v_j is the L_{CRC} bits in CRC hash results.

After the calculation of CRC based codeword self check is completed, the components of codeword are complete,

Algorithm 1 Codeword Generation

Input:$message$, BL, L_{HASH}, L_{CRC}, R, $Salt$, $Seed$
Output:$C \leftarrow \{\}$
1 $D \leftarrow$ group into blocks($message$, BL)
2 $modulated\_sections \leftarrow NULL$
3 $salt \leftarrow Salt \oplus Seed$
4 **For** D_i in D **do**
5 $j \leftarrow \left\lfloor \frac{i}{R-1} \right\rfloor \times R + (i-1)\ \%\ R + 1$
6 **append** D_i to $modulated\_sections$
7 $h_j \leftarrow L_{HASH}$ bits of HASH ($salt$ // $modulated\_sections$ // $salt$)
8 $C_j \leftarrow$ append h_j to D_i
9 **append** h_j to $modulated\_sections$
10 **append** C_j to C
11 **If** i mod R == 0 **Then**
12 $C_{j+1} \leftarrow (L_{Codeword} - L_{CRC})$ bits of HASH($salt$ //$modulated\_sections$//$salt$)
13 **append** C_{j+1} to C
14 $modulated\_sections \leftarrow NULL$
15 **End if**
16 **End**
17 **For** C_j in C **do**
18 $C_j \leftarrow$ append L_{CRC} bits of CRC32 ($salt$ // C_j // $salt$) to C_j
19 **End**
Return C

and the codeword C_j can be obtained by combination. The alg. 1 describes the process from secret message to codeword, which includes two parts: Message grouping and codeword generation. In the process of calculating hash summary and CRC hash value, salt adding operation is carried out to ensure the randomness of verification information.

2) Demodulation Phase: The description of CRC based codeword self check demodulation phase is shown in alg. 2. For candidate symbols, only if they meet the verification rules can they be exported as candidate codewords. In the demodulation process, the CRC check value is recalculated to judge whether it is consistent with the v'_j part of the codeword, and if not, it will be discarded directly. In the demodulation process, the method of adding salt and its value are consistent with the modulation process.

C. Mapping Matrix Checking Method Based on XOR

At the same time, the number of columns in the matrix is adjustable, which is conducive to reduce the interference of continuous packet loss noise.

1) Modulation Phase: The mapping matrix and XOR check in the matrix are shown in Fig.12, and the data packet number fills the matrix in row order. For the $m-th$ mapping matrix, the matrix starts with $O_{\tau+1}$, where τ is defined by Eq. 7. The row number M_{rows} of the matrix is related to the range of the symbol. M_{rows} is calculated by Eq. 6 according to $L_{Codeword}$.

$$M_{rows} = 2^{L_{Codeword}} \tag{6}$$

$$\tau = M_{cols} \times (m-1) \times M_{rows} \tag{7}$$

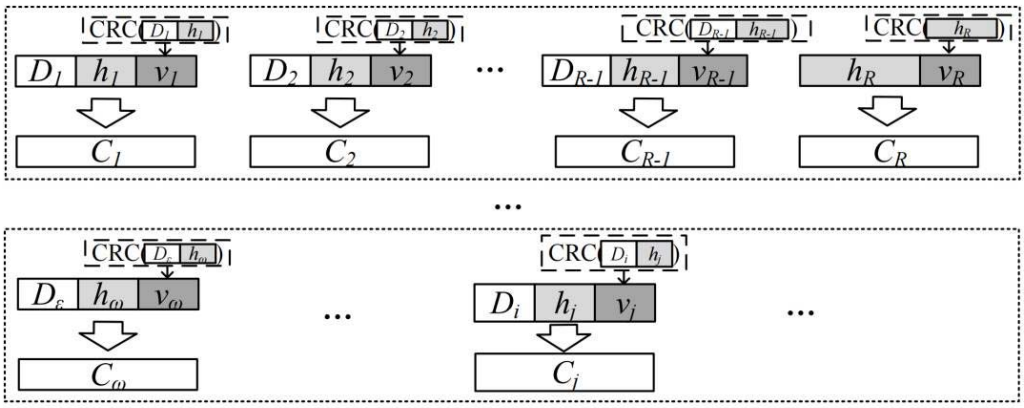


Fig. 11. Codeword self-check based on CRC during the modulation phase.

Algorithm 2 Effective Codeword Identification

Input:S', L_{CRC}, $Salt$, $Seed$
Input:$C' \leftarrow \{\}$
1 $salt \leftarrow Salt \oplus Seed$
2 **For** $\{S'_j\}$ in S' **do**
3 $\{C'_j\} \leftarrow \{\}$
4 **For** S'_j in $\{S'_j\}$ **do**
5 $v'_j,\ h'_j,\ D'_j \leftarrow$ extracted from S'_j
6 $crc32\_result \leftarrow L_{CRC}$ bits of CRC32 ($salt$ // D'_j // h'_j // $salt$)
7 **If** $v'_j == crc32\_result$
8 **append** S'_j to $\{C'_j\}$
9 **End if**
10 **End**
11 **append** $\{C'_j\}$ to C'
12 **Return** C'

Algorithm 3 Codeword Converted to Sequence

Input:C, $L_{Codeword}$, M_{cols}, $Salt$, $Seed$
Output:$P \leftarrow \{\}$
1 $S \leftarrow \{\}$
2 $offset \leftarrow$ Random ($Salt \oplus Seed$)
3 **For** C_j in C **do**
4 $S_k \leftarrow$ Integer (C_j) + 1
5 **append** S_k to S
6 **If** j mod 2 == 0
7 append ($S_k \oplus S_{k-1}$) to S
8 **End if**
9 **End**
10 **For** S_k in S **do**
11 $offset \leftarrow$ Random ($offset$)
12 $S_k \leftarrow (S_k + offset)\ mod\ (2^{L_{Codeword}}) + 1$
13 **End**
14 **For** S_k in S **do**
15 $P_k \leftarrow P_k\ (k,\ S_k)$
16 **append** P_k to P
17 **End**
18 **Return** P

$$P_k\ (k, S_k) = \left\lfloor \frac{k-1}{M_{cols}} \right\rfloor \times (M_{rows} \times M_{cols}) + M_{cols} \times (S_k - 1) + (k-1)\ \%\ M_{cols} + 1 \quad (8)$$

In the mapping matrix, each packet number has its coordinate value, the ordinate represents the symbol, and the abscissa represents the grouping sequence number. The check is based on the check of two symbols in the data matrix. As shown in Fig.12, the XOR value $S_{(m-1)\times M_{cols}+1} \oplus S_{(m-1)\times M_{cols}+2}$ of the first two groups of symbols need to be added. The XOR relation requires $M_{cols}\ \%3 = 0$ for every 3 symbols, so that the mapping matrix is synchronized with the XOR cycle.

The conversion process from codeword to packet serial number, such as algorithm alg. 3, The input parameters include codeword set, transmission parameter and random number seed. The first step is to add XOR check, the second step is to add random offset, the third step is to convert the symbol to serial number, and each step corresponds to a cycle.

The input parameters include codeword set, transmission parameter and random number seed. The first step is to add XOR check, the second step is to add random offset, and the third step is to convert the symbol to serial number. The three steps correspond to a cycle.

The first step is to add XOR check. When judging whether it is going to the even group, the first two groups of symbols XOR are added to the symbol set s. The second step is to add a random offset, each iteration of pseudo-random number generator, so that even if the same symbol, the corresponding processing results are not the same. In the third step, the symbol is mapped to the serial number, and the symbol and group number constitute the $[K, S_K]$ binary, which is converted into the packet serial number according to the Eq. 8.

2) Demodulation Phase: In the demodulation process, the symbol information is extracted according to the mapping matrix, and the XOR check symbol is verified. The receiver obtains the packet loss sequence number P', calculates the group number according to Eq. 9, and extracts candidate symbols by Eq. 10. Under the influence of noise, the candidate symbols of each group are not unique, so the results are

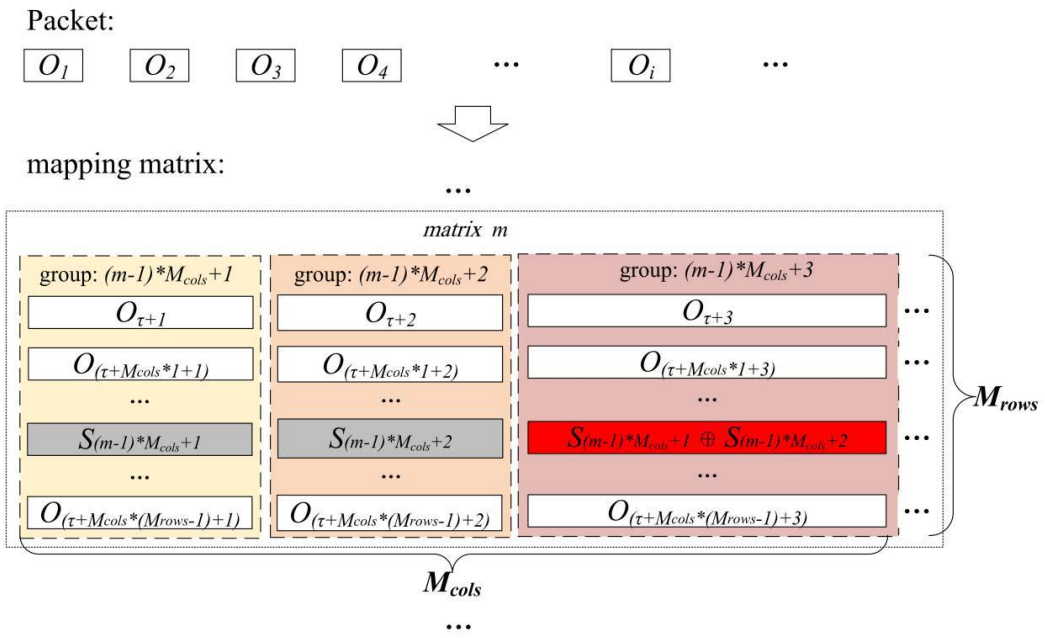


Fig. 12. The phase of mapping matrix and XOR check: The check is based on the inter-codeword verification in the data matrix.

$$\{\{S'_1, \cdots\}, \{S'_2, \cdots\}, \cdots, \{S'_k, \cdots\}, \cdots\}.$$

$$k = \left\lfloor \frac{P'}{M_{rows} \times M_{cols}} \right\rfloor \times M_{cols} + (P' - 1) \ \% \ M_{cols} + 1 \tag{9}$$

$$S'_j = \left\lfloor \frac{P'_j - M_{rows} \times M_{cols} \times \left\lfloor \frac{P'_j}{M_{rows} \times M_{cols}} \right\rfloor - 1}{M_{cols}} \right\rfloor \tag{10}$$

$$S'_j = (S'_j - offset \ \% \ (2^{L_{Codeword}}) + 2^{L_{Codeword}}) \ \% \ (2^{L_{Codeword}}) + 1 \tag{11}$$

For the candidate symbols, the random offset is eliminated first, which is shown in Eq. 11. The offsets of each group are obtained by the iterative pseudo-random number generator, which is the same as the modulation phase. By verifying the XOR relationship between symbols, the first layer of multi-layer verification can be completed. In the verification process, using the characteristic of XOR relation, when the symbols S'_1, S'_2, S'_3 satisfy $S'_1 \oplus S'_2 \oplus S'_3 = 0$, it is judged that they conform to the verification rules.

V. Evaluation

The covert timing channel evaluation based on multi-stage verification and error correction consists of four parts: undetectability test, robustness test, transmission performance test and construction cost test. The undetectability test is composed of IPD detection, continuous packet loss detection and interval packet loss detection. The robustness test mainly evaluates the average Bit Error Rate (BER) of CTC in various communication scenarios with different parameters. Transmission performance tests evaluate the transmission rate under different parameter configuration, test the data transmission ability of covert timing channel.

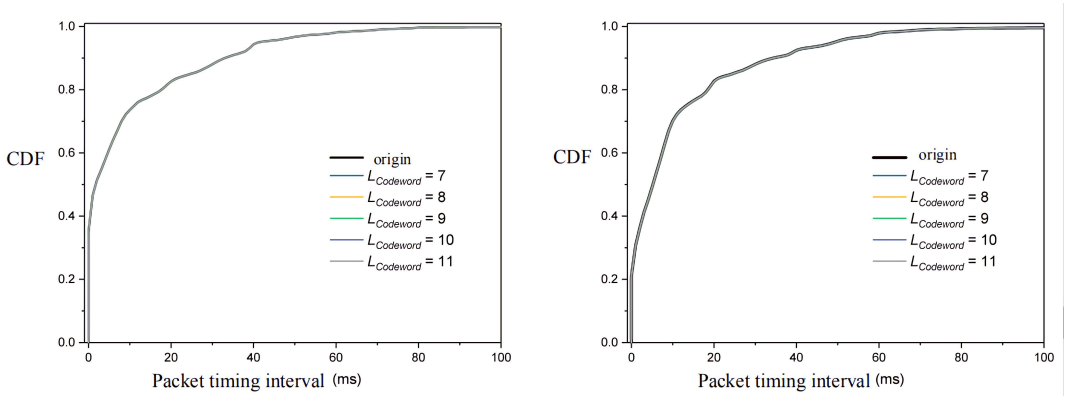
TABLE I
The Table of Test Environment Information

Type	Information
PC platform	i5-9400, DDR4 16GB
Software	Windows 7, QT 5.9.5, python 3.6, Ubuntu 16.04, mysql 5.7
Dataset	VoLTE captured test result, random noise

A. Dataset and Parameters

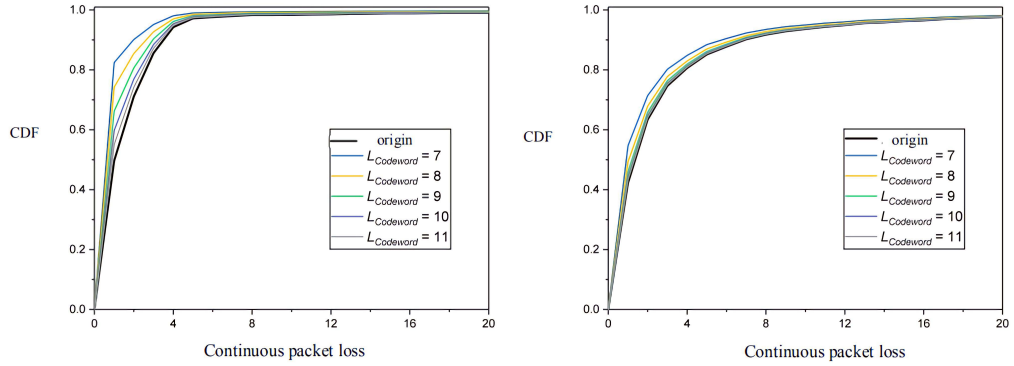
The parameters of the covert timing channel include $L_{Codeword}$, L_{HASH}, L_{CRC}, R and M_{cols}. The $L_{Codeword}$ determines the CTC's active packet loss density. L_{HASH} and L_{CRC} are closely correlated with robustness, which represent the number of hash check blocks embedded in codewords and CRC check blocks embedded in codewords respectively. The parameter R represents the inter symbol check reset period based on hash, which affects the demodulation efficiency. The parameter M_{cols} is the number of columns in the mapping matrix, and the complexity of the relationship between sequence number and symbol is positively related to the number of columns.

The software and hardware environment of the evaluation experiment is shown in TABLE I. All the data are stored in the MySQL database, and the modulation and demodulation results are obtained through the covert timing channel processing logic based on QT. According to the modulation and demodulation results, the undetectability is evaluated. Based on Python script, the packet capture results are restored to video data, and the video quality before and after modulation is evaluated, and the test results of covert channel construction cost are obtained. In addition, in order to effectively evaluate the robustness and compare the BER levels under various dropout rates, four kinds of random noises with packet loss rates of 0.5%, 1%, 2% and 5% are generated.



(a) CDF under scenario-Excellent (b) CDF under scenario-Good

Fig. 13. CDF of the packet timing interval distribution.



(a) CDF under the scenario-Excellent (b) CDF under the scenario-Good

Fig. 14. CDF of continuous packet loss.

TABLE II
THE PARAMETER VALUE RANGE OF THE COVERT TIMING CHANNEL DURING TESTS

Parameter name	Value range
$L_{Codewrod}$	7, 8, 9, 10, 11
L_{HASH}	2, 3, 4, 5
L_{CRC}	2, 3, 4, 5
R	1, 2, 3
M_{cols}	9, 18, 27, 36, 45

TABLE III
SUMMARY OF IPD DETECTION RATE

$L_{Codeword}$	Method	Detection rate
7, 8, 9, 10, 11	K-S test	0 %
	Welchs t test, Mann-Whitney rank test[1]	0 %
	K-L divergence	0 %
	Wasserstein distance	0 %
	Energy distance	0 %

[1] Pass either Welchs t test or Mann-Whitney rank test

The test parameters of the covert timing channel are shown in TABLE II. The relationship among $L_{Codeword}$, L_{HASH}, L_{CRC} and BL is shown in Eq. 1.

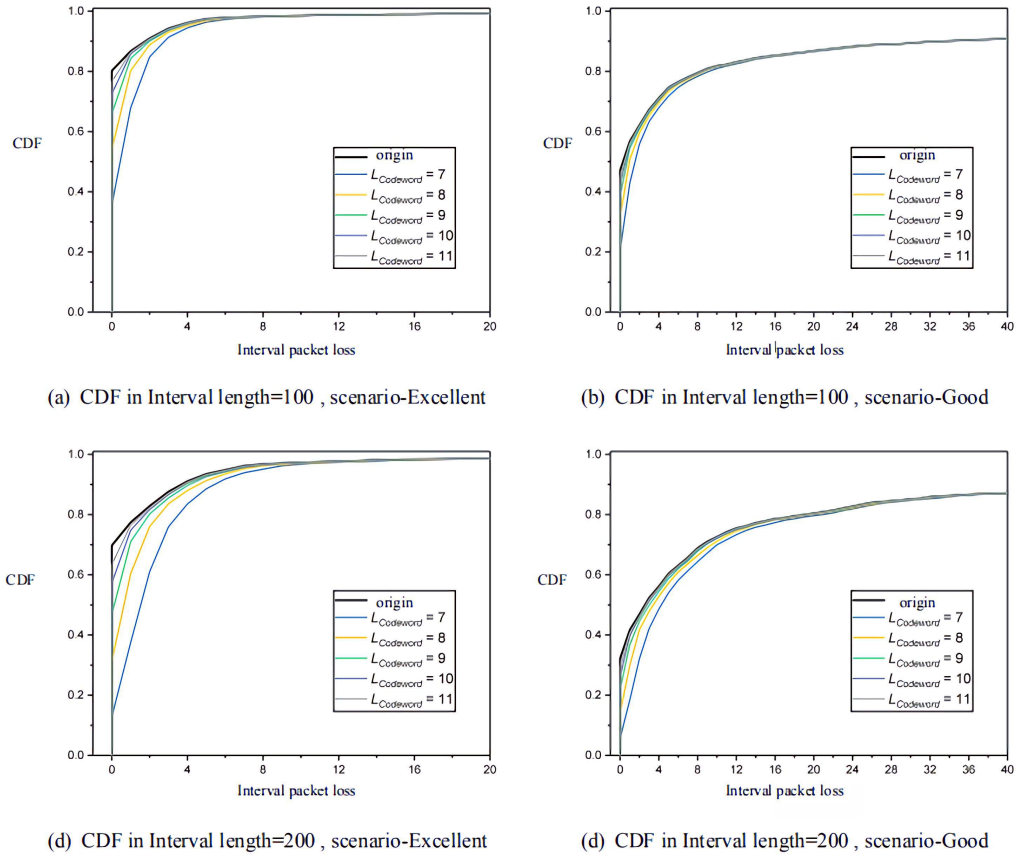
B. Undetectability

The undetectability test covers IPD distribution, interval packet loss number distribution and continuous packet loss number distribution. Four different types of detection tools are used, including CDF detection, distribution consistency test, K-L divergence and relative distance. According to the summary mode in TABLE III, the final detection conclusion is obtained. Since the active dropout rate is determined by the parameter $L_{Codeword}$, the undetectability evaluation is based on different $L_{Codeword}$ parameters.

1) IPD Testing: The CDF curve of IPD distribution is shown in Fig.13. The covert timing channel has no effect on CDF distribution. When the active packet loss rate of the covert timing channel decreases, the impact on the IPD distribution decreases, and the CDF curve can no longer detect the difference.

The quantitative evaluation results of IPD distribution detection are shown in TABLE III. The covert timing channel cannot be detected through IPD distribution. The current covert timing channel detection methods are mostly based on IPD distribution characteristics, so they have good undetectability. Because the active packet loss rate of the covert channel is less than 1%, it has enough concealment.

2) Continuous Packet Loss Detection: The main difference between the two scenarios is the proportion of continuous



(a) CDF in Interval length=100 , scenario-Excellent

(b) CDF in Interval length=100 , scenario-Good

(d) CDF in Interval length=200 , scenario-Excellent

(d) CDF in Interval length=200 , scenario-Good

Fig. 15. CDF of interval packet loss number.

packet loss. In this method, active packet loss produces discrete packet loss with length of 1. As shown in Fig.14, the curve of excellent scene deviates, while the curve of good scene is basically consistent. Due to the weak network noise in excellent scenario, the average dropout rate is $\leq$ 1%, and the covert timing channel has influence on the curve; the average packet loss rate of good scene has reached about 10%, while the active packet loss rate of covert timing channel is less than 1%, so there is no impact.

The quantitative evaluation results of continuous packet loss detection are shown in TABLE IV. Good scenario has good concealment. When $L_{Codeword} \geq 7$, all the detection are passed. In the excellent scenario, only when the parameter $L_{Codeword}$ is greater than or equal to 9 can all detection items be passed. Therefore, in order to ensure that the covert timing channel has the ability of full scene immunity detection, the parameter Lcodeword should be $L_{Codeword} \geq 9$.

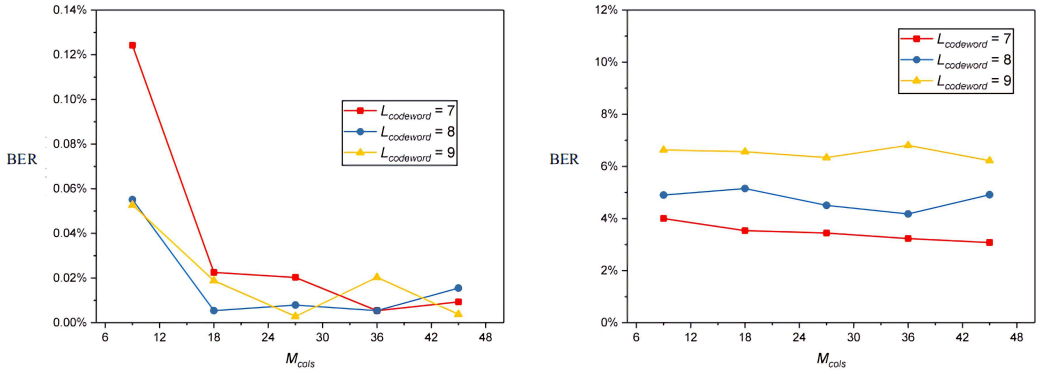
3) Interval Packet Loss Detection: In the covert timing channel based on active packet loss, there is packet loss behavior in the fixed interval, which affects the number of interval packet loss. The CDF curve of interval packet loss is shown in Fig.15, and the interval length is set to 100 and 200. As shown in Fig.15(a) and Fig.15(c), the CDF curve of covert timing channel has deviated, and the relative deviation increases with the decrease of $L_{Codeword}$. Good scenario is shown in Fig.15(b) and Fig.15(d). The relative deviation of covert timing channel is smaller and has better concealment.

TABLE IV
DETECTION RATE SUMMARY OF CONTINUOUS PACKET LOSS DETECTION

Scenario	$L_{Codeword}$	Method	Detection rate
Excellent	7, 8	K-L divergence	100 %
	9, 10, 11	K-L divergence	0 %
	7, 8, 9, 10, 11	Wasserstein distance	0 %
	7, 8, 9, 10, 11	Energy distance	0 %
Good	7, 8, 9, 10, 11	K-L divergence	0 %
	7, 8, 9, 10, 11	Wasserstein distance	0 %
	7, 8, 9, 10, 11	Energy distance	0 %

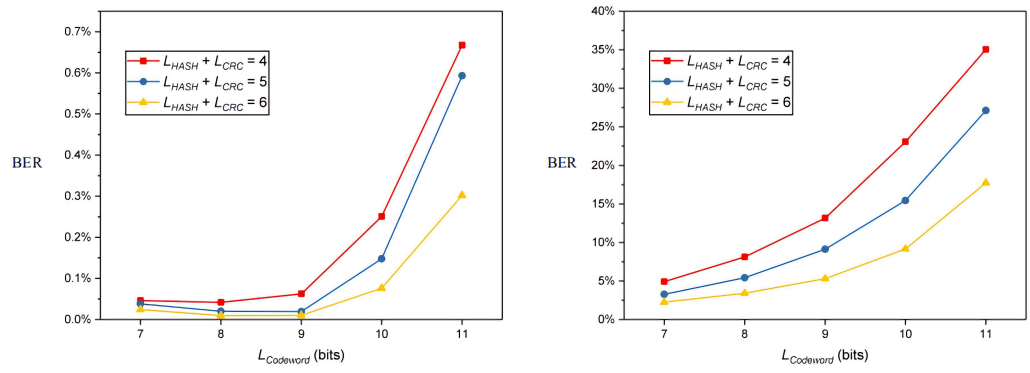
The quantitative evaluation results of interval packet loss detection are shown in TABLE V. In excellent scenario, when $L_{Codeword} \geq 8$, the covert timing channel can pass the detection; in good scenario, when $L_{Codeword} \geq 9$, the covert timing channel passes all detection; when $L_{Codeword} = 8$, the covert timing channel has a high probability of passing the detection.

4) Summary of Undetectability Test: The detection rate of covert channel in this time is summarized in TABLE VI. In good scenario, this method has good concealment, and it still has a high probability of passing the detection when $L_{Codeword} = 8$. To pass all tests in all scenarios, the parameter $L_{Codeword}$ should be $L_{Codeword} \geq 9$.



(a) average BER in scenario-Excellent (b) average BER in scenario-Good

Fig. 16. The relationship between the average BER and M_{cols}.



(a) average BER in scenario-Excellent (b) average BER in scenario-Good

Fig. 17. The relationship between the average BER and $L_{Codeword}$.

TABLE V

DETECTION RATE SUMMARY OF INTERVAL PACKET LOSS DETECTION

Scenario	$L_{Codeword}$	Method	Detection rate
Excellent	7	Wasserstein distance	100 %
	8, 9, 10, 11	Wasserstein distance	0 %
	7	Energy distance	100 %
	8, 9, 10, 11	Energy distance	0 %
Good	7	Wasserstein distance	100 %
	8	Wasserstein distance	30 %
	9, 10, 11	Wasserstein distance	0 %
	7	Energy distance	100 %
	8	Energy distance	30 %
	9, 10, 11	Energy distance	0 %

TABLE VI

COVERT TIMING CHANNEL DETECTION RATE SUMMARY BASED ON MULTI-STAGE VERIFICATION AND ERROR CORRECTION

Scenario	$L_{Codeword}$				
	7	8	9	10	11
Excellent	100 %	100 %	0 %	0 %	0 %
Good	100 %	30 %	0 %	0 %	0 %

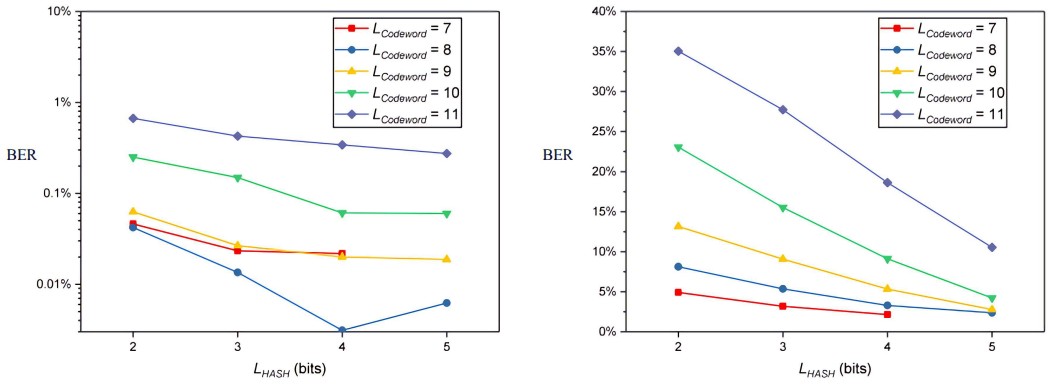
C. Robustness Test

The evaluation index of robustness test is bit error rate. In the covert timing channel, the parameters affecting BER include $L_{Codeword}$, L_{HASH}, L_{CRC}, R and M_{cols}, so the robustness evaluation mainly focuses on these five parameters. In terms of test data set, in addition to excellent scenario and good scenario, four different proportions of random packet loss scenarios are also set.

The average bit error rate in excellent and good scenarios is shown in Fig.16, Fig.17, Fig.18, Fig.19 and Fig.20. Fig.16 shows the relationship between average bit error rate and parameter M_{cols}. In Fig.16(a), the BER level in excellent scenario is already low, and increasing M_{cols} can reduce the average bit error rate to a certain extent. In Fig.16(b), the BER level in good scenario is high, and the effect of increasing M_{cols} is limited.

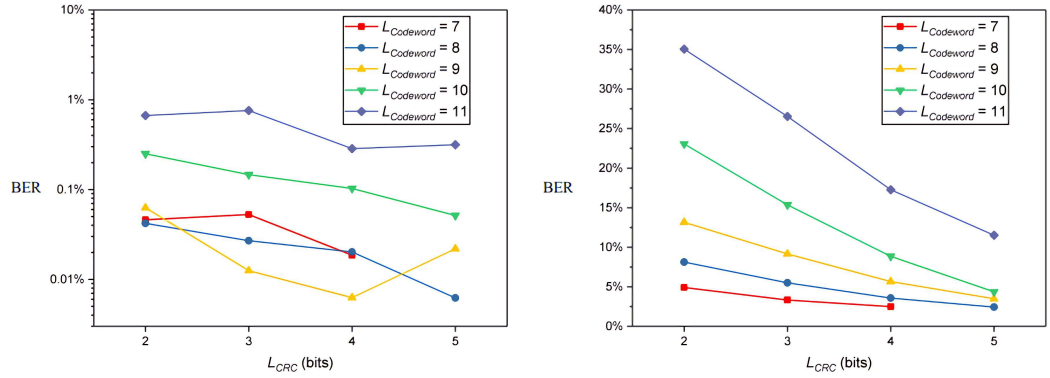
In Fig.17, when $L_{HASH} + L_{CRC}$ remains unchanged, increasing $L_{Codeword}$ leads to a growth in BER. Since the quantity of packets corresponding to $L_{Codeword}$ bits data is $2^{L_{Codeword}}$, the number of packets doubles with the increase of 1 bit of $L_{Codeword}$, and the noise intensity of each group is also doubled under the same packet loss rate. Therefore, in order to achieve better robustness, the parameter $L_{Codeword}$ should be reduced as much as possible.

In Fig.18, the average BER decreases with the growth of L_{HASH}, and the improvement effect of average bit error rate in good scene is better. Similarly, in Fig.19, the average bit error rate decreases with the increase of L_{CRC}. In excellent scenario, the average bit error rate has been at a low level, and the effect of increasing L_{HASH} and L_{CRC} is limited; in good



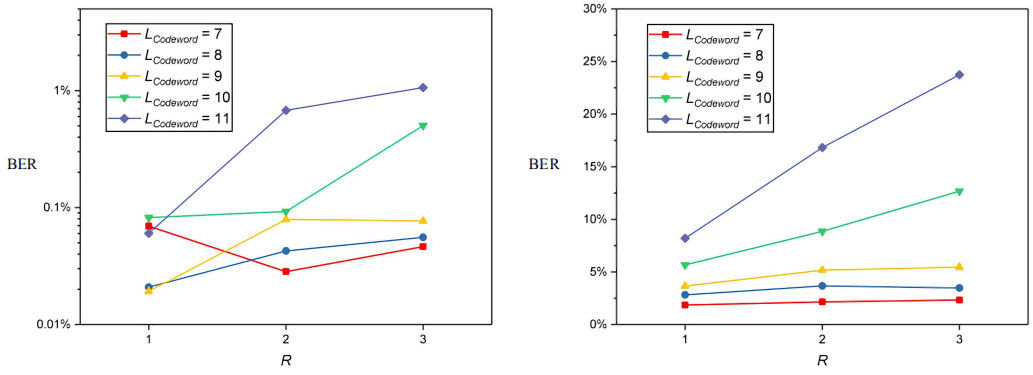
(a) average BER in scenario-Excellent (b) average BER in scenario-Good

Fig. 18. The relationship between the average BER and L_{HASH}.



(a) average BER in scenario-Excellent (b) average BER in scenario-Good

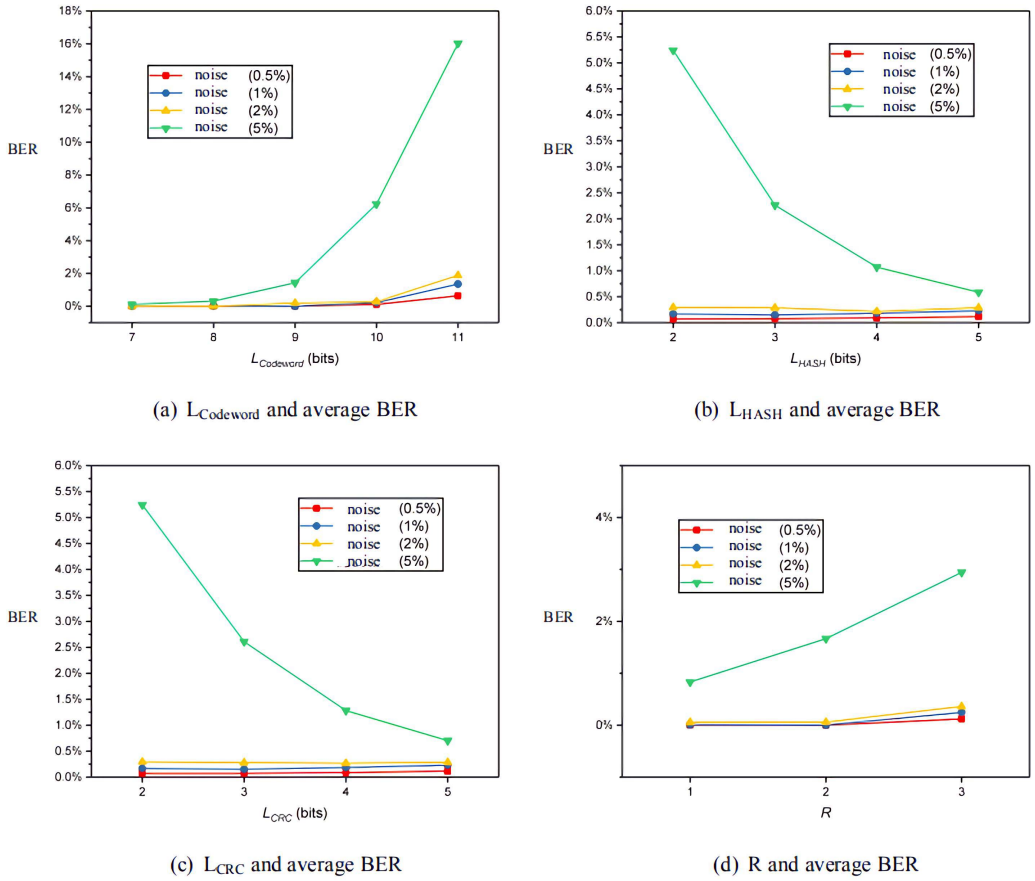
Fig. 19. The relationship between the average BER and L_{CRC}.



(a) average BER in scenario-Excellent (b) average BER in scenario-Good

Fig. 20. The relationship between the average BER and R.

scenario, with the increase of $L_{HASH} + L_{CRC}$, the average bit error rate decreases rapidly. On the other hand, increasing $L_{Codeword}$ to a certain extent can accommodate more parity bits in the codeword, so it has a positive significance in improving robustness. In Fig.20, the average bit error rate increases with the increase of parameter R. Since R determines the reset period of hash based inter symbol check, the larger R is, the longer the reset period is, and the greater the effect of noise accumulation on robustness. In the random noise scenario, the results of robustness test are in Fig.21. In Fig.21, when random packet loss rate is less than 2%, the average bit error rate changes slightly, which proves that the robust



(a) $L_{Codeword}$ and average BER (b) L_{HASH} and average BER

(c) L_{CRC} and average BER (d) R and average BER

Fig. 21. The relationship among average bit error rate and parameters in random noise scene.

method is sufficient to deal with the noise impact. When the random packet loss noise is 5%, the average bit error rate curve fluctuates with the change of parameters.

Through the test of the two modes, the bit error rate can be reduced by increasing M_{cols}, decreasing $L_{Codeword}$, increasing L_{HASH}, increasing L_{CRC} and decreasing R. According to Eq. 1, the number of data bits BL contained in each codeword is closely related to the length of codeword, hash check digit L_{HASH} and CRC check digit L_{CRC}. The improvement of robustness has an impact on the detection ability and transmission performance. The parameter configuration needs to be considered comprehensively.

D. Transmission Performance Test

According to the design scheme of the covert timing channel, the parameters $L_{Codeword}$, L_{HASH}, L_{CRC} and R all affect the transmission performance. The relationship between covert timing channel capacity and parameters is shown in Eq. 12, and the relationship between transmission rate and parameters of covert timing channel is shown in Eq. 13.

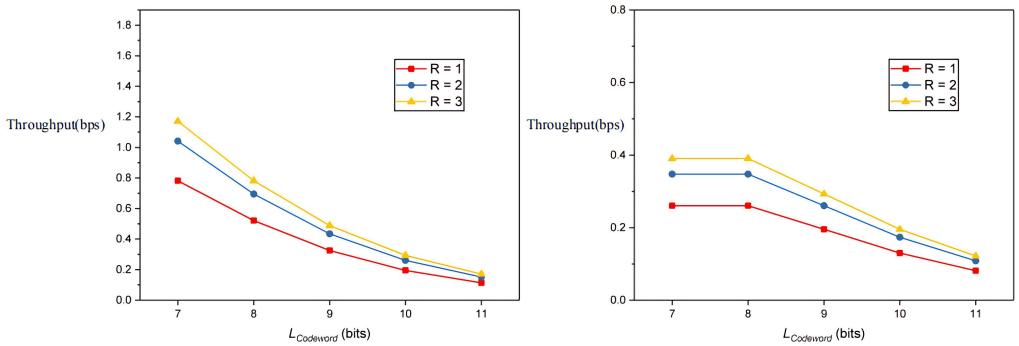
$$\begin{aligned} Capacity &= \frac{BL \times R}{(R+1) \times 2^{L_{Codeword}}} \times \frac{2}{3} \quad (bpp) \\ &= \frac{(L_{Codeword} - L_{HASH} - L_{CRC}) \times R}{(R+1) \times 2^{L_{Codeword}}} \\ &\quad \times \frac{2}{3} \quad (bpp) \end{aligned} \tag{12}$$

$$\begin{aligned} Throughput &= Capacity \times 100 \times \frac{2}{3} \quad (bps) \\ &= \frac{(L_{Codeword} - L_{HASH} - L_{CRC}) \times R}{(R+1) \times 2^{L_{Codeword}}} \\ &\quad \times 100 \times \frac{2}{3} \quad (bps) \end{aligned} \tag{13}$$

When $L_{HASH} + L_{CRC} = 4$, the relationship between the transmission rate of covert timing channel and $L_{Codeword}$ and R is shown in Fig.22 (a). When $L_{HASH} + L_{CRC} = 6$, the relationship between the transmission rate of covert timing channel and $L_{Codeword}$ and R is shown in Fig.22 (b). In the excellent scenario, the transmission performance can reach 1.0 bps. By increasing the reset period R, the transmission rate can be improved at a certain level, but it is far less than the performance improvement brought by reducing $L_{HASH} + L_{CRC}$.

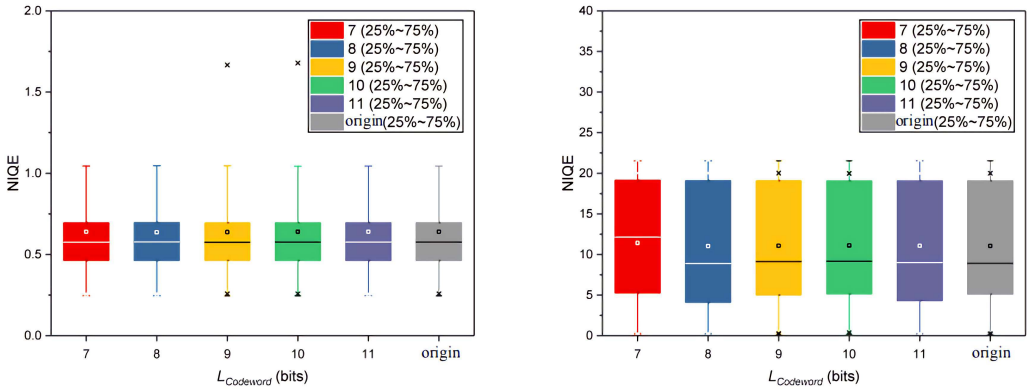
E. Build Cost Test

The construction cost test of the CTC mainly evaluates the impact of the CTC in the field of video quality. The evaluation index adopts the non reference index of NIQE (Natural Image Quality Evaluator) [27], and the NIQE value is negatively correlated with the video quality. The NIQE evaluation results of covert timing channel are shown in Fig.23. Due to the difference of network noise intensity in the two scenarios, the video quality has been greatly different. Fig.23 (a), in the



(a) Throughput when $L_{HASH}+L_{CRC}=4$ (b) Throughput when $L_{HASH}+L_{CRC}=6$

Fig. 22. The relationship among transmission rate of CTC and $L_{Codeword}$ and R.



(a) NIQE in scenario-Excellent (a) NIQE in scenario-Excellent

Fig. 23. NIQE evaluation results of CTC.

excellent scenario, the NIQE values under different $L_{Codeword}$ are similar, and the fluctuation is small. Fig.23(b), in the good scenario, the covert timing channel causes the fluctuation of NIQE value, but there is no significant difference in distribution. By comparing Fig.23 (a) and Fig.23 (b), compared with the video quality loss caused by covert timing channel, the impact of network noise on video quality loss is greater, so the construction cost of the covert timing channel is acceptable.

F. Summary of Test Results

Via the evaluations including the undetectability, robustness, transmission performance and construction cost of the covert timing channel, each parameter has an impact on the index. In practical application, the covert timing channel should have better robustness and transmission performance on the basis of ensuring the concealment of transmission, so it is necessary to config. parameters reasonably. According to the test results, when $L_{Codeword} \geq 9$, it can meet the requirements of undetectability. On the contrary, as a parasitic channel, CTC is inevitably disturbed by noise. Therefore, in the comprehensive evaluation, the acceptable bit error rate in excellent scenario is set to be less than 0.1% and that in good scenario is less than 1%, and then the parameter combination is screened.

The comprehensive evaluation results of the covert timing channel are shown in TABLE VII. By comparing the test results, the better parameter configurations in excellent and good scenarios are selected. It is illustrated from the table that better capacity can be achieved by sacrificing certain robustness in the excellent scenario. In good scenario, more robust information is needed to resist noise interference, so the transmission reliability can be guaranteed by sacrificing performance.

TABLE VIII compares the performance and bit error rate of several covert timing channels, namely SCC [28], AFTC [29], coco [30], SPCC [31], and MSV-CTC (Multi-stage verification Covert Timing Channel)-the scheme in this paper. It can be seen that although this method loses some performance, it is more robust than other covert timing channels.

According to the results of undetectability test, robustness test, transmission performance test and robustness test, this method can meet the requirements of covert timing channel. Due to the active packet loss modulation, the covert timing channel has good concealment in the detection method based on IPD. After adjusting the parameter $L_{Codeword}$, it passes the test based on the number of continuous packet loss and interval packet loss. By combining multiple levels of check and error correction, the CTC effectively improves the transmission robustness and reduces the bit error rate level.

TABLE VII

COMBINATION EVALUATION ON MSV-CTC

Scenario	M_{cols}	$L_{Codeword}$	L_{HASH}	L_{CRC}	R	Packet rate(avg.)	BER(avg.)
Excellent	36	9	3	2	2	0.35 bps	< 0.001 %
	27	9	2	3	3	0.40 bps	< 0.02 %
	27	9	2	2	3	0.49 bps	< 0.08 %
Good	45	9	5	2	1	0.13 bps	< 0.85 %
	36	10	5	3	3	0.10 bps	< 0.10 %
	45	10	5	4	2	0.05 bps	< 0.01 %

TABLE VIII

THROUGHPUT AND CAPACITY COMPARISONS AMONG THE PROPOSED SCHEME AND OTHER SIMILAR WORKS

Scheme	Throughput	Capacity	BER
SCC[28]		0.2$\sim$ 0.8 bpp	2 %
AFTC[29]		0.5 bpp	4 %
CoCo[30]		0.1$\sim$ 0.5 bpp	4 %
SPCC[31]	0.7$\sim$ 3 bps		0.9 %
MSV-CTC	0.49 bps	0.005 bpp	0.08 %

By adjusting the combination of transmission parameters, when the transmission performance reaches 0.49 bps, the bit error rate level is not higher than 0.08%, reaching the basic level of covert timing channel.

VI. RELATED WORKS

The security issues of data transmission and storage have been addressed in the recent researches [32]–[35]. Literatures have discussed the implementation of covert timing channel in wireless networks. Kiyavash and Coleman [36] implemented the IPD covert timing channel in the CSMA/CA protocol with trigger mechanism. Radhakrishnan *et al.* [37] implemented a scheme named covert DCF under IEEE 802.11 network. Yue *et al.* [38] demonstrated their covert channel technology through existing network services, ICMP pings commands and Trojan chat applications. Edwards *et al.* [39] proposed the legitimate application of wireless time covert channel, and proposed using covert timing channel to mitigate threats caused by the wormhole attacks under the mobile ad-hoc networks.

In addition, there are also some special methods in the research of CTC building methods. Some schemes embed secret information by changing transmission bit rate [40], [41]; some schemes encode secret information by active packet loss [42]; some schemes conduct covert communication by cache consistency vulnerability [43]; some schemes hide secret information by retransmission mechanism of some protocols [44], and construct time covert channel by queue scheduling [45]. There are also some methods to mix covert timing channel with covert storage channel [46]. These methods are beneficial exploration for the research of CTC building methods, It also provides a enlightenment on the construction method of covert channel in this paper.

VII. CONCLUSION

The data transmission and communication security of IoT-enabled MTS is challenged by various threats. This paper introduces the construction method of CTC based on multi-stage verification, focusing on reducing the transmission error rate and mitigating the threats from critical data leakage. To enhance the reliability of CTC, the method adopts multi-stage verification and error correction mode, including inter symbol check based on hash, codeword self check based on CRC and mapping matrix check based on XOR. The experimental evaluation results reveal that the CTC can reduce the bit error rate and guarantee the transmission performance by flexibly organizing the transmission parameters on the premise of ensuring the concealment of transmission. In the excellent scenario, when the BER is $\leq$0.08%, the transmission performance is kept at 0.49 bps. In the good scenario with strong network noise, although this method loses some performance, it can still maintain the transmission performance of 0.2 bps under the condition of bit error rate less than 1%, which effectively proves the effectiveness of multi-stage verification and error correction.

In terms of confidentiality, salt is added in the process of hash value calculation by combining user shared information and random fields in RTP header. At the same time, random offsets are added to each group of symbols by iterative pseudo-random number generator. So that even if the same data, the packet loss position at different time is not exactly the same. On the other hand, even if the listener knows the transmission principle, due to the lack of key information such as transmission parameters, the complexity of reverse cracking is high, and the hidden message is protected. For active listeners, only by resetting all the fields related to the serial number can the covert timing channel be blocked completely. Therefore, the CTC building method based on multi-stage verification can meet the requirements of covert timing channel index in the fields of stealthiness, reliability, confidentiality, modulation cost and transmission performance. There is still room for improvement in the field of robustness. Under the extreme data transmission environment such as high dropout rate, the decoder cannot extract the secret message even if the CRC code has been applied. In the future, we plan to add rateless code, such as fountain code during the message grouping phase and recombination phase so as to mitigate the limitation in extreme data transmission environment.

REFERENCES

[1] A. Voliotis, S. Oikonomou, and I. Filippopoulos, "An integrated maritime cyber security policy proposal," in *Proc. ISER 637th Int. Conf. Sci., Technol., Eng. Manage. (ICSTEM)*, Crete, Greece, Aug. 2019, pp. 1–9.

[2] Y. M. Amin and A. T. Abdel-Hamid, "Classification and analysis of IEEE 802.15.4 PHY layer attacks," in *Proc. Int. Conf. Sel. Topics Mobile Wireless Netw. (MoWNeT)*, Apr. 2016, pp. 1–8.

[3] C. Wang, C. Zhang, B. Wu, Y. Tan, and Y. Wang, "A novel anti-detection criterion for covert storage channel threat estimation," *Sci. China Inf. Sci.*, vol. 61, no. 4, pp. 212–214, 2018.

[4] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[5] F. Qiao, J. Wu, J. Li, A. Bashir, S. Mumtaz, and U. Tariq, "Trustworthy edge storage orchestration in intelligent transportation systems using reinforcement learning," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4443–4456, Jul. 2021.

[6] Q. Zhang *et al.*, "A hierarchical group key agreement protocol using orientable attributes for cloud computing," *Inf. Sci.*, vol. 480, pp. 55–69, Apr. 2019.

[7] X. Yu, Y.-A. Tan, Z. Sun, J. Liu, C. Liang, and Q. Zhan, "A fault-tolerant and energy-efficient continuous data protection system," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 8, pp. 2945–2954, 2018.

[8] C. Wang, D. Wang, G. Xu, and D. He, "Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0," *Sci. China Inf. Sci.*, vol. 65, no. 1, pp. 1–15, Jan. 2022.

[9] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Trans. Depend. Sec. Comput.*, early access, Sep. 8, 2020, doi: 10.1109/TDSC.2020.3022797.

[10] D. Wang, X. Zhang, Z. Zhang, and P. Wang, "Understanding security failures of multi-factor authentication schemes for multi-server environments," *Comput. Secur.*, vol. 88, Jan. 2020, Art. no. 101619.

[11] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, "Understanding node capture attacks in user authentication schemes for wireless sensor networks," *IEEE Trans. Depend. Sec. Comput.*, early access, Feb. 17, 2020, doi: 10.1109/TDSC.2020.2974220.

[12] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network Protocols," *IEEE Commun. Surveys Tuts.*, vol. 9, no. 3, pp. 44–57, 3rd Quart., 2007.

[13] N. B. Lucena, G. Lewandowski, and S. J. Chapin, "Covert channels in IPv6," in *Privacy Enhancing Technologies*, G. Danezis and D. Martin, Eds. Berlin, Germany: Springer, 2006, pp. 147–166.

[14] X. Luo, E. W. W. Chan, and R. K. C. Chang, "TCP covert timing channels: Design and detection," in *Proc. IEEE Int. Conf. Dependable Syst. Netw.*, Jun. 2008, pp. 420–429.

[15] Y. Li, X. Zhang, X. Xu, and Y.-A. Tan, "A robust packet-dropout covert channel over wireless networks," *IEEE Wireless Commun.*, vol. 27, no. 3, pp. 60–65, Jun. 2020.

[16] Q. Zhang, X. Zhang, Y. Xue, and J. Hu, "A stealthy covert storage channel for asymmetric surveillance VoLTE endpoints," *Future Gener. Comput. Syst.*, vol. 102, pp. 472–480, Jan. 2020.

[17] D. D. Dhobale, V. R. Ghorpade, B. S. Patil, and S. B. Patil, "Steganography by hiding data in TCP/IP headers," in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng.(ICACTE)*, Aug. 2010, pp. V4-61–V4-65.

[18] D. M. Dakhane and P. R. Deshmukh, "Active warden for TCP sequence number base covert channel," in *Proc. Int. Conf. Pervas. Comput. (ICPC)*, Jan. 2015, pp. 1–5.

[19] X. Zhang, L. Guo, Y. Xue, and Q. Zhang, "A two-way VoLTE covert channel with feedback adaptive to mobile network environment," *IEEE Access*, vol. 7, pp. 122214–122223, 2019.

[20] W. Mazurczyk, M. Karaś, K. Szczypiorski, and A. Janicki, "YouSkyde: Information hiding for Skype video traffic," *Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13521–13540, 2016.

[21] Y. Li, S. Yao, K. Yang, Y.-A. Tan, and Q. Zhang, "A high-imperceptibility and histogram-shifting data hiding scheme for JPEG images," *IEEE Access*, vol. 7, pp. 73573–73582, 2019.

[22] J. Kaur, S. Wendzel, and M. Meier, "Countermeasures for covert channel-internal control protocols," in *Proc. 10th Int. Conf. Availability, Rel. Secur.*, Aug. 2015, pp. 422–428.

[23] M. A. Elsadig and Y. A. Fadlalla, "Network protocol covert channels: Countermeasures techniques," in *Proc. 9th IEEE-GCC Conf. Exhib. (GCCCE)*, May 2017, pp. 1–9.

[24] Y.-A. Tan, X. Zhang, K. Sharif, C. Liang, Q. Zhang, and Y. Li, "Covert timing channels for IoT over mobile networks," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 38–44, Dec. 2018.

[25] R. Archibald and D. Ghosal, "A covert timing channel based on fountain codes," in *Proc. IEEE 10th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Jun. 2012, pp. 970–977.

[26] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[27] L. Zhang, L. Zhang, and A. C. Bovik, "A feature-enriched completely blind image quality evaluator," *IEEE Trans. Image Process.*, vol. 24, no. 8, pp. 2579–2591, Aug. 2015.

[28] Y. Liu, D. Ghosal, F. Armknecht, A.-R. Sadeghi, S. Schulz, and S. Katzenbeisser, "Robust and undetectable steganographic timing channels for i.i.d. traffic," in *Information Hiding*, R. Böhme, P. W. L. Fong, and R. Safavi-Naini, Eds. Berlin, Germany: Springer, 2010, pp. 193–207.

[29] W. Liu, G. Liu, J. Zhai, Y. Dai, and D. Ghosal, "Designing analog fountain timing channels: Undetectability, robustness, and model-adaptation," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 4, pp. 677–690, Apr. 2016.

[30] A. Houmansadr and N. Borisov, "Coco: Coding-based covert timing channels for network flows," in *Information Hiding*, T. Filler, T. Pevný, S. Craver, and A. Ker, Eds. Berlin, Germany: Springer, 2011, pp. 314–328.

[31] X. Zhang, Y.-A. Tan, C. Liang, Y. Li, and J. Li, "A covert channel over VoLTE via adjusting silence periods," *IEEE Access*, vol. 6, pp. 9292–9302, 2018.

[32] Z. Xu *et al.*, "Decentralized opportunistic channel access in CRNs using big-data driven learning algorithm," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 5, no. 1, pp. 57–69, Feb. 2021.

[33] K. Lou, Y. Yang, E. Wang, Z. Liu, T. Baker, and A. Bashir, "Reinforcement learning based advertising strategy using crowdsensing vehicular data," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4635–4647, Jul. 2021.

[34] K. Zrar Ghafoor *et al.*, "Millimeter-wave communication for internet of vehicles: Status, challenges, and perspectives," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8525–8546, Sep. 2020.

[35] X. Zhang, C. Liang, Q. Zhang, Y. Li, J. Zheng, and Y.-A. Tan, "Building covert timing channels by packet rearrangement over mobile networks," *Inf. Sci.*, vols. 445–446, pp. 66–78, Jun. 2018.

[36] N. Kiyavash and T. Coleman, "Covert timing channels codes for communication over interactive traffic," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Apr. 2009, pp. 1485–1488.

[37] S. V. Radhakrishnan, A. S. Uluagac, and R. Beyah, "Realizing an 802.11-based covert timing channel using off-the-shelf wireless cards," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 722–728.

[38] M. Yue, W. H. Robinson, L. Watkins, and C. Corbett, "Constructing timing-based covert channels in mobile networks by adjusting CPU frequency," in *Proc. 3rd Workshop Hardw. Architectural Support Secur. Privacy*, Jun. 2014, pp. 2:1–2:8.

[39] J. J. Edwards, J. D. Brown, and P. C. Mason, "Using covert timing channels for attack detection in MANETs," in *Proc. MILCOM IEEE Mil. Commun. Conf.*, Oct. 2012, pp. 1–7.

[40] H. Tian, J. Sun, C.-C. Chang, J. Qin, and Y. Chen, "Hiding information into voice-over-IP streams using adaptive bitrate modulation," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 749–752, Apr. 2017.

[41] P. M. B. Harley, M. Tummala, and J. C. McEachen, "High-throughput covert channels in adaptive rate wireless communication systems," in *Proc. Int. Conf. Electron., Inf., Commun. (ICEIC)*, Jan. 2019, pp. 1–7.

[42] W. Mazurczyk, "Lost audio packets steganography: The first practical evaluation," *Secur. Commun. Netw.*, vol. 5, no. 12, pp. 1394–1403, Dec. 2012.

[43] F. Yao, M. Doroslovački, and G. Venkataramani, "Covert timing channels exploiting cache coherence hardware: Characterization and defense," *Int. J. Parallel Program.*, vol. 47, no. 4, pp. 595–620, Aug. 2019.

[44] W. Mazurczyk, M. Smolarczyk, and K. Szczypiorski, "Retransmission steganography and its detection," *Soft Comput.*, vol. 15, no. 3, pp. 505–515, Mar. 2011.

[45] A. Ghassami, X. Gong, and N. Kiyavash, "Capacity limit of queueing timing channel in shared FCFS schedulers," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 789–793.

[46] G. Xu, W. Yang, and L. Huang, "Hybrid covert channel in LTE—A: Modeling and analysis," *J. Netw. Comput. Appl.*, vol. 111, pp. 117–126, Jun. 2018.

Chen Liang received the B.S. degree in electrical engineering and the Ph.D. degree in computer science and technology from Beijing Institute of Technology in 2014 and 2020, respectively. He has been an Associate Professor with Beijing Information Science and Technology University. His research interests include information security and coding theory.

Thar Baker (Senior Member, IEEE) received the Ph.D. degree in autonomic cloud applications from Liverpool John Moores University (LJMU) in 2010. He was a Reader of cloud engineering with the Department of Computer Science, LJMU, from 2013 to 2019. He is currently an Associate Professor with the Department of Computer Science, University of Sharjah, Sharjah, United Arab Emirates. He has published numerous refereed research articles in multidisciplinary research areas, including: cloud computing, big data, algorithm design, intelligent transportation systems, and autonomic routing.

Raheel Nawaz is currently the Chair and the Director of the Business Transformations Research Centre. He is also the Director of Digital Technology Solutions, and the Head of Text and Data Mining Lab and the Apprenticeships Research Unit, Manchester Metropolitan University, where he holds the Personal Chair of applied artificial intelligence. In the past, he has founded and/or headed research units specializing in artificial intelligence, data science, digital transformations, digital education, and apprenticeships in higher education. He has led on several funded research projects in the U.K., EU, South Asia, and Middle East. He has held adjunct or honorary positions with prestigious research, higher education, and policy organizations, both in the U.K. and overseas. He has briefed the U.K. and Pakistani Parliamentarians on numerous occasions, and regularly makes media appearances speaking on a range of topics, especially artificial intelligence and higher education.

Yuanzhang Li received the B.S., M.S., and Ph.D. degrees in software and theory of computer from Beijing Institute of Technology in 2001, 2004, and 2015, respectively. He has been an Associate Professor with Beijing Institute of Technology. His research interests include mobile computing and information security.

Yu-An Tan received the B.S., M.S., and Ph.D. degrees in software and theory of computer from Beijing Institute of Technology, in 1991, 1994, and 2004, respectively. Since 2010, he has been a Professor and a Ph.D. Supervisor with Beijing Institute of Technology. His research interests include information security, network storage, and embedded systems.